

UNITED STATES DISTRICT COURT

for the
Eastern District of PennsylvaniaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)electronic communications (both sent & received,
opened & unopened) and stored materials and
documents in the account mail3412@aol.com

Case No. 18-1298-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, LOCATION TO BE SEARCHED, incorporated by reference

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein.

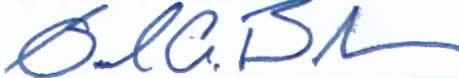
The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § § 513, 1028(a),
1028A, 1343, 1344, 371 and
42 U.S.C. § 408

Offense Description
Uttering counterfeit securities, identity fraud, aggravated identity theft, wire fraud,
bank fraud, conspiracy and social security fraud.

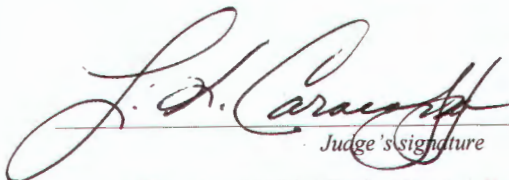
The application is based on these facts:
See Attached Affidavit.☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Samuel A. Bracken, Postal Inspector, USPIIS

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/10/2018City and state: Philadelphia, PA

Judge's signature

LINDA K. CARACAPPA, Chief U.S. Magistrate Judge

Printed name and title

ATTACHMENT A – LOCATION TO BE SEARCHED

(To be served on Oath Inc.)

This warrant applies to information associated with the Oath Inc. user ID and/or email address:

- **mall3412@aol.com**

Which is stored at premises owned, maintained, controlled, and/or operated by Oath Inc., headquartered at 22000 AOL Way Dulles VA 20166.

ATTACHMENT B

(These two pages to be served on Oath Inc.)

I. Information to be disclosed by Oath Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period of June 1, 2016 to the present:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and
- f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 7 days of the issuance of this warrant.

II. Production of Files

Copies of the above-described records and stored information should be obtained from original storage and provided by the following means:

- On CD-R (CD-Recordable) or other appropriate digital media, and delivered or mailed to United States Postal Inspector Samuel A. Bracken within 7 days of the issuance of this warrant.

ITEMS TO BE SEIZED BY THE GOVERNMENT

(These Two Pages Not to be Served on Oath Inc.)

Agents for the government may search the materials produced by Oath Inc. for the following items:

All information for the time period of June 1, 2016 to the present as described below that constitutes evidence of violations of 18 U.S.C. § 513 – Uttering Counterfeit Securities; 18 U.S.C. § 1028A – Aggravated Identity Theft; 18 U.S.C. § 1028(a) – Identity Fraud; 18 U.S.C. § 1343 – Wire Fraud; 18 U.S.C. § 1344 – Bank Fraud; 18 U.S.C. § 371 – Conspiracy to commit offenses against the United States; and 42 U.S.C. § 408 – Social Security Fraud, that is:

- (a) Any and all messages regarding travel plans and itineraries; check cashing; counterfeit checks; bank account information; store and bank visits; division of proceeds; and counterfeit identification.
- (b) Receipts, letters, emails, and other correspondence from various airline, vehicle rental, hotel and motel locations in the United States, or other such information that show travel to locations in the United States.
- (c) Use of identity information, to include names; dates of birth; Social Security numbers; driver's license or state-issued identification information.
- (d) Evidence indicating how and when the email account was accessed or used.
- (e) Information indicating the identity of the users and/or creators of the subject account.
- (f) Information showing the identity of the person(s) who communicated with the user IDs listed in Attachment A about matters relating to the identity theft scheme

set forth in the Affidavit and its Exhibit A, including coconspirators known and unknown to the government, including records that help reveal their whereabouts.

- (g) Information concerning how any identity information was acquired; about the gathering and distribution of any goods, profits, or proceeds from the scheme described in the affidavit; and evidence of the use of identifying information, to include receipts, transactional statements, and order information.

ATTACHMENT A – LOCATION TO BE SEARCHED

(To be served on Oath Inc.)

This warrant applies to information associated with the Oath Inc. user ID and/or email address:

- **mall3412@aol.com**

Which is stored at premises owned, maintained, controlled, and/or operated by Oath Inc., headquartered at 22000 AOL Way Dulles VA 20166.

ATTACHMENT B

(These two pages to be served on Oath Inc.)

I. Information to be disclosed by Oath Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period of June 1, 2016 to the present:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and
- f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within 7 days of the issuance of this warrant.

II. Production of Files

Copies of the above-described records and stored information should be obtained from original storage and provided by the following means:

- On CD-R (CD-Recordable) or other appropriate digital media, and delivered or mailed to United States Postal Inspector Samuel A. Bracken within 7 days of the issuance of this warrant.

ITEMS TO BE SEIZED BY THE GOVERNMENT

(These Two Pages Not to be Served on Oath Inc.)

Agents for the government may search the materials produced by Oath Inc. for the following items:

All information for the time period of June 1, 2016 to the present as described below that constitutes evidence of violations of 18 U.S.C. § 513 – Uttering Counterfeit Securities; 18 U.S.C. § 1028A – Aggravated Identity Theft; 18 U.S.C. § 1028(a) – Identity Fraud; 18 U.S.C. § 1343 – Wire Fraud; 18 U.S.C. § 1344 – Bank Fraud; 18 U.S.C. § 371 – Conspiracy to commit offenses against the United States; and 42 U.S.C. § 408 – Social Security Fraud, that is:

- (a) Any and all messages regarding travel plans and itineraries; check cashing; counterfeit checks; bank account information; store and bank visits; division of proceeds; and counterfeit identification.
- (b) Receipts, letters, emails, and other correspondence from various airline, vehicle rental, hotel and motel locations in the United States, or other such information that show travel to locations in the United States.
- (c) Use of identity information, to include names; dates of birth; Social Security numbers; driver's license or state-issued identification information.
- (d) Evidence indicating how and when the email account was accessed or used.
- (e) Information indicating the identity of the users and/or creators of the subject account.
- (f) Information showing the identity of the person(s) who communicated with the user IDs listed in Attachment A about matters relating to the identity theft scheme

set forth in the Affidavit and its Exhibit A, including coconspirators known and unknown to the government, including records that help reveal their whereabouts.

- (g) Information concerning how any identity information was acquired; about the gathering and distribution of any goods, profits, or proceeds from the scheme described in the affidavit; and evidence of the use of identifying information, to include receipts, transactional statements, and order information.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, SAMUEL A. BRACKEN, United States Postal Inspector, United States Postal Inspection Service, being duly sworn, depose and state as follows:

1. I am a United States Postal Inspector assigned to the Philadelphia Division of the United States Postal Inspection Service ("Inspection Service"), and have been so employed since February 2004. I am currently assigned to the Miscellaneous Crimes Team, which investigates violations of federal law including identity fraud, theft of mail, aggravated identity theft, mail fraud and wire fraud, in violation of Title 18, United States Code, Sections 1028(a), 1708, 1028A, 1341 and 1343, respectively. I have received training in investigating identity theft, credit card fraud, wire fraud and mail fraud offenses, including attending seminars and conferences hosted by the International Association of Financial Crimes Investigators. During my employment as a Postal Inspector, I have participated in hundreds of investigations involving identity fraud, theft of mail, aggravated identity theft, mail fraud and wire fraud. In addition, I have been the Inspection Service's case agent on numerous investigations involving these offenses.

PURPOSE OF AFFIDAVIT

2. I submit this affidavit in support of an application for a warrant, pursuant to Title 18, United States Code, Section 2703, to search the electronic communications contained in the email account below controlled by Oath Inc.:

- **mall3412@aol.com**

3. On May 4, 2018, the Honorable Marilyn Heffley, United States Magistrate Judge, issued warrants to search nine email accounts, including the account above, for evidence of violations of 18 U.S.C. §§ 513, 1028(a), 1028A, 1343, 1344, 371 and 42 U.S.C. § 408. I was the

affiant on the application for those warrants; a copy of my affidavit as executed May 4, 2018 is attached hereto as Exhibit A. I have reviewed Exhibit A and it remains true and correct to the best of my knowledge, information and belief, with the addition of the facts set out below.

4. In my May 4, 2018 affidavit, the provider for the email account above, **mall3412@aol.com**, was listed as Oath Holdings, Inc. The search warrant and application for search warrant were directed to Oath Holdings, Inc., and stated that the location to be searched was in the Northern District of California.

5. After Magistrate Judge Heffley approved the email search warrants on May 4, 2018, your affiant received materials from the providers for six of the other email addresses, but received no materials in connection with the warrant for **mall3412@aol.com**.

6. On August 2, 2018, your affiant received an email from a representative of Oath, Inc., stating that Oath, Inc. would not obey the search warrant concerning **mall3412@aol.com**, because it was addressed to the wrong provider. As explained by the Oath, Inc. representative, Verizon purchased Yahoo, Inc. and merged Yahoo, Inc. with AOL. The Oath, Inc. representative continued that while Oath Holdings, Inc. was the successor company for Yahoo email accounts, Oath, Inc. was the successor company for AOL accounts (such as **mall3412@aol.com**). In addition, the Oath, Inc. representative stated that the AOL account information was located at 22000 AOL Way in Dulles, Virginia, not in Sunnyvale, California. Dulles, Virginia is located within the Eastern District of Virginia.

7. The Oath, Inc. representative also informed me that AOL has preserved the content of **mall3412@aol.com** based on the search warrant signed by Magistrate Judge Heffley on May 4, 2018.

8. Accordingly, your affiant seeks a warrant to search the AOL email account **mall3412@aol.com**, for evidence of violations of 18 U.S.C. §§ 513, 1028(a), 1028A, 1343, 1344, 371 and 42 U.S.C. § 408. As set out in my original affidavit, which is attached as Exhibit A, ¶¶ 16-32, there is probable cause that this email account has been used by Ahmad Becoate in furtherance of a nationwide counterfeit check scheme targeting Walmart.

9. In addition, two of the email accounts for which Magistrate Judge Heffley approved warrants on May 4, 2018 were for accounts belonging to Ahmad Becoate. Analysis of the material obtained through the searches of Becoate's other two email accounts showed that Becoate's accounts contained personal identifying information (PII), including PII that has been used in presenting and cashing counterfeit checks at Walmart locations; hotel receipts from locations near Walmart stores where counterfeit checks were cashed; and communications with co-conspirators sharing PII. Becoate's other two emails are **ahmadbecoate@gmail.com** and **crazyswagg87@gmail.com**.

10. More recently, on July 10, 2018, a grand jury sitting in this district returned an indictment against Ahmad Becoate and five others, which remains under seal. Becoate is the lead defendant on the sealed indictment, which charges that beginning no later than June 2016 and continuing until at least May 2018, Becoate and others conspired and schemed to present thousands of counterfeit payroll checks, with a face value of more than \$700,000, at Walmart stores located across the United States.

11. Finally, I have been informed by Walmart, specifically, Darick Leighty, Global Investigator for Walmart, that as recently as July 21, 2018, Ahmad Becoate passed a counterfeit payroll check at a Walmart located in Burlington, North Carolina. The basis for Leighty's

identification of Becoate was a video image. Thus it appears that Becoate has continued his fraudulent scheme.

CONCLUSION

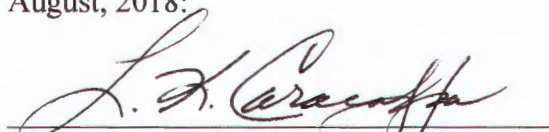
12. Based on the foregoing, I submit that there is probable cause that the items set forth in Attachment B2, which constitute evidence and instrumentalities of violations of 18 U.S.C. § 513 – uttering counterfeit securities; 18 U.S.C. § 1028 – credit card fraud; 18 U.S.C. § 1028A – aggravated identity theft; 18 U.S.C. § 1343 – wire fraud; 18 U.S.C. § 1344 – bank fraud; 18 U.S.C. § 371 – conspiracy to commit offenses against the United States (i.e., wire fraud, bank fraud, credit card fraud and uttering counterfeit securities); and 42 U.S.C. § 408 – Social Security fraud, are located in the aforementioned email account, which is hosted on servers owned, maintained, and/or operated by Oath Inc., headquartered at 22000 AOL Way, Dulles, Virginia 20166.

13. Based upon the above stated information, I respectfully request that this Court issue a warrant to search the subject email account, and that such search warrant be directed to Oath Inc. for the purpose of searching the aforementioned email account.



SAMUEL A. BRACKEN
US Postal Inspector
US Postal Inspection Service

Sworn to before me this 10th day of
August, 2018:



HONORABLE LINDA K. CARACAPPA
CHIEF UNITED STATES MAGISTRATE JUDGE

EXHIBIT A

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, SAMUEL A. BRACKEN, United States Postal Inspector, United States Postal Inspection Service, being duly sworn, depose and state as follows:

1. I am a United States Postal Inspector assigned to the Philadelphia Division of the United States Postal Inspection Service ("Inspection Service"), and have been so employed since February 2004. I am currently assigned to the Miscellaneous Crimes Team, which investigates violations of federal law including identity fraud, theft of mail, aggravated identity theft, mail fraud and wire fraud, in violation of Title 18, United States Code, Sections 1028(a), 1708, 1028A, 1341 and 1343, respectively. I have received training in investigating identity theft, credit card fraud, wire fraud and mail fraud offenses, including attending seminars and conferences hosted by the International Association of Financial Crimes Investigators. During my employment as a Postal Inspector, I have participated in hundreds of investigations involving identity fraud, theft of mail, aggravated identity theft, mail fraud and wire fraud. In addition, I have been the Inspection Service's case agent on numerous investigations involving these offenses.

PURPOSE OF AFFIDAVIT

2. I submit this affidavit in support of applications for warrants, pursuant to Title 18, United States Code, Section 2703, to search the electronic communications contained in the following nine email accounts controlled by Oath Holdings Inc. and Google Inc.:

AHMAD BECOATE EMAIL ADDRESSES:

- **ahmadbecoate@gmail.com (Google)**
- **Mall3412@aol.com (Oath Holdings)**
- **Crazyswagg87@gmail.com (Google)**

JEFFREY ROACH EMAIL ADDRESSES:

- **j_black009@yahoo.com (Oath Holdings)**
- **Jeffreyroach1985@gmail.com (Google)**

JETHRO RICHARDSON EMAIL ADDRESS:

- **Jax.black51@yahoo.com (Oath Holdings)**

JARED MILLER EMAIL ADDRESSES:

- **Jlmiller1286@gmail.com (Google)**
- **Mochaboy69@gmail.com (Google)**

JUQUAN HARVEY EMAIL ADDRESS:

- **juquananthony@gmail.com (Google)**

along with certain subscriber and log records associated with these email accounts as described in Attachments A1 and A2, which are attached to this affidavit and incorporated by reference. The email accounts that are the subject of this search warrant application are controlled by Oath Holdings Inc., 701 First Avenue, Sunnyvale, CA 94089, and Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043. This application seeks warrants to search the aforementioned email accounts ("the subject accounts") for evidence, fruits and instrumentalities of violations of 18 U.S.C. § 513 – uttering counterfeit securities; 18 U.S.C. § 1028(a) – identity fraud; 18 U.S.C. § 1028A – aggravated identity theft; 18 U.S.C. § 1343 – wire fraud; 18 U.S.C. § 1344 – bank fraud; 18 U.S.C. § 371 – conspiracy to commit offenses against the United States (i.e., wire fraud, bank fraud, identity fraud and uttering counterfeit securities); and 42 U.S.C. § 408 – Social Security fraud and to seize such evidence, fruits and instrumentalities of these crimes.

3. Unless otherwise stated, the information contained in this affidavit is either personally known to me or has been related to me by others, including other law enforcement agents and officers, and/or obtained via review of various documents and records as more particularly described below. Since this affidavit is being submitted for the limited purpose of

securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause to believe that fruits, instrumentalities and evidence of violations of federal law will be found within the email accounts that are the subject of this affidavit.

INTRODUCTION

4. Along with special agents of the United States Secret Service ("USSS") and the United States Social Security Administration, Office of Inspector General ("SSA-OIG"), I'm investigating the activities of a group of individuals who have been engaged in a nationwide identity theft and counterfeit check cashing scheme since at least June 2016, which activity, at least by several subjects, has continued until the present. As explained in detail below, our investigation has shown that subjects Ahmad BECOATE, Jeffrey ROACH, Jethro RICHARDSON, Jared MILLER and Juquan HARVEY have conspired with others known and unknown to pass counterfeit checks at Walmarts across the United States, including in the Eastern District of Pennsylvania, using stolen and fraudulent bank account and identification information. In order to carry out their scheme, the subjects have traveled throughout the country on commercial airlines and in rental vehicles. They have also stayed at various chain hotels throughout the country. They have provided the above email addresses to the airline, car rental and hotel companies so that those companies can contact them for reservation information, hotel updates, and booking receipts. Accordingly, based on the information outlined in this affidavit, as well as my training and experience, your affiant has probable cause to believe that the above email accounts are being used by subjects BECOATE, ROACH, RICHARDSON, MILLER, HARVEY and others in connection with the above-described scheme.

5. Based upon the information set forth in this affidavit, there is probable cause to believe that the nine subject email accounts identified in paragraph 2 above contain certain items, set forth more fully in Attachments B1 and B2, which constitute fruits, instrumentalities, and evidence of violations of 18 U.S.C. § 513 – uttering counterfeit securities; 18 U.S.C. § 1028(a) – identity fraud; 18 U.S.C. § 1028A – aggravated identity theft; 18 U.S.C. § 1343 – wire fraud; 18 U.S.C. § 1344 – bank fraud; 18 U.S.C. § 371 – conspiracy to commit offenses against the United States (i.e., wire fraud, bank fraud, identity fraud and uttering counterfeit securities); and 42 U.S.C. § 408 – Social Security fraud.

THE SUBJECT EMAIL AND INTERNET SERVICE ACCOUNT PROVIDERS

6. Oath Holdings Inc. and Google, Inc. are publicly traded companies, located in the United States, that manufacture computer software and also provide internet based online programs such as free internet searches, email, and other services. Oath Holdings Inc. is headquartered at 701 First Avenue, Sunnyvale, CA 94089, and Google, Inc. is headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

7. Based on my training and past experience with electronic evidence, I know the following about Google Inc. and Oath Holdings Inc.

- Subscribers obtain an account by registering on the Internet with Oath Holdings Inc. or Google Inc. Subscribers provide a name, location and a desired login name and password, and users are prompted to provide a secondary email address; however, a secondary email address is not required to create an account. The information provided by a user is not verified by Oath Holdings Inc. or Google Inc.;

- Oath Holdings Inc. and Google Inc. maintain electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information;
- Subscribers to these services may access their accounts on servers maintained and owned by Oath Holdings Inc. and Google Inc. from any computer connected to the Internet located anywhere in the world;
- Any email that is sent to a subscriber is stored in the subscriber's "mail box" on Oath Holdings Inc. or Google Inc. servers until the subscriber deletes the email. If the message is not deleted by the subscriber and the subscriber accesses the account periodically, that message can remain on Oath Holdings Inc. or Google Inc. servers indefinitely;
- When the subscriber sends an email, it is initiated at the user's computer, transferred via the internet to Oath Holdings Inc. and Google Inc. servers, and then transmitted to its end destination. Users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from Oath Holdings Inc.'s or Google Inc.'s server, the email can remain on the system indefinitely. The sender can delete the stored email message, thereby eliminating it from the email box maintained by Oath Holdings Inc. or Google Inc., but that message will remain in the recipient's email box unless the recipient deletes it as well, or unless the recipient's account is subject to account size limitations;

- Subscribers can store files, including emails and image files, on servers maintained and owned by Oath Holdings Inc. or Google Inc.;
- A subscriber to Oath Holdings Inc. or Google Inc. need not store copies on his/her home computer of emails and image files stored in his/her account. The subscriber may store emails and other files on Oath Holdings Inc.'s or Google Inc.'s server for which there is insufficient storage space in the subscriber's computer and which he/she does not wish to maintain on the computer at his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on Oath Holdings Inc.'s or Google Inc. server;
- Both Oath Holdings Inc. and Google Inc. offer a "Contacts" folder for users. Email and contact information for associates, businesses, and friends may be added to the address book by the subscriber.

DESCRIPTION OF INVESTIGATION

WALMART

8. Since approximately June 2016, thousands of counterfeit payroll checks have been cashed or attempted to be cashed by BECOATE, ROACH, RICHARDSON, MILLER, and HARVEY at dozens of Walmart locations in more than 35 states. The subjects have acquired the personal identifying information of numerous individuals, to include their names, dates of birth, and Social Security numbers, and have used this information to obtain or create fraudulent identification cards. With this information, the subjects have used the information to defraud Walmart by presenting counterfeit payroll checks bearing the names of compromised individuals. These counterfeit payroll checks contain bank account and bank routing numbers

which were also misappropriated. The bank routing numbers are the routing numbers of legitimate banks; certain of the bank account numbers are the account numbers of legitimate businesses, not the businesses that appear as payors on the counterfeit checks. Based on the investigation to date, I estimate that the subjects have caused Walmart to sustain an actual loss of at least approximately \$494,297 and an intended loss of at least approximately \$831,743.

9. Walmart permits customers to cash payroll checks at most Walmart stores. When payroll checks are presented to store employee by the customer, the store employee will scan the check through a check reader. The customer is also required to enter the customer's Social Security Number ("SSN") into a keypad. The payroll check routing number and account number, along with the SSN and any other information provided by the customer, are then transmitted through and interstate wire communication from the retail store's computer system to Fidelity National Information Services ("FIS") computer servers in Chicago, Illinois or St. Petersburg, Florida.

10. In this case, the bank account number of Southeastern Pennsylvania Transportation Authority ("SEPTA") and the routing number of SEPTA's bank, PNC Bank, were used to cash and attempt to cash counterfeit payroll checks on at least ninety-seven (97) occasions. SEPTA's headquarters are located at 1234 Market Street, Philadelphia, PA, within the Eastern District of Pennsylvania.

11. Additionally, at least 34 of these fraudulent payroll checks were cashed or were attempted to be cashed at Walmart locations in the Eastern District of Pennsylvania in such locations as Eddystone, PA; Allentown, PA; Reading, PA; Quakertown, PA and Pottstown, PA. As detailed above in paragraph 10, the transaction of cashing the check or attempting to cash the check initiates an interstate wire communication beginning at the point of sale terminal at the

Walmart store location, to various servers outside of the state of Pennsylvania for approval or denial. Once a decision is made to accept the check for cashing or deny it, an interstate wire communication is transmitted back to the Walmart location within the Eastern District of Pennsylvania to the same terminal that initiated the transaction.

12. An employee of Walmart working in security, Investigator Darick Leighty, has provided federal investigators with numerous surveillance videotapes, and photographs obtained from those videotapes, of counterfeit checks being cashed at Walmarts throughout the United States, which videotapes and photographs depict activities at various Walmarts beginning in November 2016. Your affiant compared the surveillance photographs and video to the driver's licenses of identified subjects in this case, BECOATE, ROACH, RICHARDSON, MILLER and HARVEY. Your affiant also compared the surveillance photographs and videos to photographs of BECOATE, ROACH, RICHARDSON, MILLER and HARVEY found on social media. Having made that comparison I can state that the surveillance videos and photographs show BECOATE, ROACH, RICHARDSON, MILLER, and HARVEY, as well as others, entering and leaving the Walmarts to cash the counterfeit checks using stolen identity information and stolen bank and routing information. I draw this conclusion for several reasons: first, because the subjects are often seen wearing the same clothing, hats, and accessories in different Walmart locations; second, in some instances, more than one of the subjects are at the same Walmart together, at the same time; third, the surveillance photographs often show the subjects checking their cellular telephones during the transactions, possibly for victim information, such as social security numbers, which information was needed to complete the transactions.

13. During this investigation, it was determined that several of the subjects had active accounts with Facebook, a social networking company that allows individuals to connect with

friends, relatives, and others. It was discovered the subjects' Facebook accounts were accessible and open to public viewing. Your affiant reviewed the Facebook profiles of ROACH, HARVEY, RICHARDSON, and MILLER and found each of these four men was Facebook friends with the other three. It should be noted that BECOATE did not have a public Facebook viewable by your affiant, but in some cases the subjects' respective Facebook pages had photographs posted with each other including photographs of BECOATE. For example, ROACH's Facebook page had photographs of ROACH with BECOATE and HARVEY and ROACH is "friends" with HARVEY, RICHARDSON, and MILLER.

COMMERICAL AIRLINE TRAVEL AND VEHICLE RENTALS

14. During this investigation, through the service of grand jury subpoenas, federal agents learned that BECOATE, ROACH, RICHARDSON, MILLER and HARVEY were using Southwest Airlines, American Airlines, and US Airways to travel across the country to various states. Soon thereafter, Walmart investigators would notice the cashing and attempting cashing of counterfeit checks at Walmarts in the state and surrounding states to which the subjects had traveled. The subjects also rented vehicles at various car rental businesses including National Car Rental, Alamo Car Rental and Enterprise Rent-a-Car. Sometimes the vehicle rentals occurred at or near the locations where the subjects lived; other times the rentals occurred at the airports to which the subjects flew. In addition, the subjects' flight and vehicle rental travel records corresponded to counterfeit check activity documented by Walmart going back to approximately June 2016.

15. In connection with almost all of the airline travel and rental car transactions, the subjects provided the airlines and car rental agencies with their personal email addresses. The airlines and car rental agencies use these email addresses for many purposes: to send email

confirmations related to reservations; email updated travel information; email itineraries; and email completed transactions and receipts. The subjects needed to access this information in order to complete their travels successfully. Information obtained in the investigation from airlines and car rental agencies concerning each of the subjects is detailed below, by subject.

AHMAD BECOATE

16. Investigation to date has shown that between December 2014 and January 2017, subject Ahmad BECOATE rented 39 vehicles from National Car Rental at various locations throughout the United States. The following information was provided to National Car Rental by or on behalf of BECOATE to secure the vehicles:

- On all rental contracts, BECOATE provided a telephone number of 267-428-6269.
- On 27 rental contracts from December 2014 to January 2016, BECOATE provided an email address of “MALL3412@AOL.COM”
- On 12 rental contracts from March 2016 to January 2017, BECOATE provided an email address of “CRAZYSWAGG87@GMAIL.COM”
- The rentals were paid with various credit and debit cards registered to BECOATE.
- On 27 rental contracts, BECOATE provided Tennessee driver's license #320-410-754 to rent the vehicles.
- On 12 rental contracts, BECOATE provided Maryland driver's license #B230-035-366-037 to rent the vehicles.

17. Your affiant conducted a query with NCIC regarding Tennessee driver's license #320-410-754 and discovered that it was non-existent. Next, I asked that a colleague, an

Inspection Service Investigative Analyst in Tennessee, query the Tennessee DMV for any license for BECOATE. Tennessee driver's license #137504227 was discovered registered to BECOATE, but that license had been revoked. The address listed on the license was 1083 Oak Street, Columbus, OH and the date of birth listed for BECOATE was February 1, 1978. Your affiant conducted a query with NCIC regarding a driver's license in Ohio for BECOATE and discovered Ohio driver's license #UB170761 registered to BECOATE at 1083 Oak Street, Apt. D, Columbus, OH. The date of birth listed on the Ohio driver's license was January 13, 1987. I conducted a query with NCIC regarding Maryland driver's license #B230-035-366-037 and found it registered to BECOATE at 5183 Clacton Avenue, Suitland, MD. The date of birth listed on the Maryland driver's license was January 13, 1987.

18. Investigation has shown that between July 2014 and February 2018, BECOATE or someone acting on his behalf made reservations for BECOATE on 45 flights on Southwest Airlines. The following information was captured by Southwest Airlines related to the flights reserved by or for BECOATE:

- The following email addresses were provided to Southwest Airlines related to flights reserved by or for BECOATE:
 - CRAZYSWAGG87@GMAIL.COM (38 times)
 - AHMADBECOATE@GMAIL.COM (7 times)
 - MALL3412@AOL.COM (once)
 - JEFFREYROACH1985@GMAIL.COM (once)
 - JLMILLER1286@GMAIL.COM (once)
- Records provided by Southwest Airlines show that reservations were made for BECOATE to fly with subject Jeffrey ROACH on five occasions. It appears

that on at least one of these occasions, ROACH's email address,

JEFFREYROACH1985@GMAIL.COM, was the email address used during booking.

- Records provided by Southwest Airlines show that reservations were made for BECOATE to fly with MILLER on three occasions. It appears that on at least one of these occasions, MILLER's email address, **JLMILLER1286@GMAIL.COM**, was the email address used during booking.

COUNTERFEIT CHECK CASHING – BECOATE

19. Investigation to date has shown that between on or about December 6, 2016 and on or about January 28, 2018, subject Ahmad BECOATE has cashed or attempted to cash approximately 600 counterfeit checks at Walmarts throughout the United States. Walmart security has provided information on checks that were cashed or attempted to be cashed, along with surveillance photographs and videotapes of the transactions. As described below, several of the counterfeit checks that were cashed or attempted to be cashed coincided with flights taken by BECOATE and vehicles rentals by BECOATE.

20. For example, on November 29, 2016, BECOATE traveled on Southwest Airlines from Baltimore-Washington International ("BWI") Airport to Dallas Love Field Airport ("Dallas Airport"). Records obtained from Southwest Airlines show that at the time of the reservation, Southwest Airlines was provided with an email address of **"CRAZYSWAGG87@GMAIL.COM."**

21. On November 29, 2016, BECOATE rented a vehicle at Dallas Love Field Airport from National Car Rental. Records obtained from National Car Rental show that at the time of

the reservation, National Car Rental was provided with an email address of "CRAZYSWAGG87@GMAIL.COM," and further that the rental was returned by BECOATE on December 9, 2016.

22. Between December 6, 2016 and December 8, 2016, approximately 41 counterfeit checks were cashed or attempted to be cashed in the name of Josh.D., James.D., and J.S., at Walmarts located in Arkansas and Texas. Your affiant has reviewed surveillance photographs of these transactions and it appears that the individual conducting those transactions was BECOATE.

23. On January 19, 2017, BECOATE rented a vehicle from National Car Rental located in Philadelphia, PA. Records obtained from National Car Rental show that at the time of the reservation, National Car Rental was provided with an email address of "CRAZYSWAGG87@GMAIL.COM." BECOATE was later arrested driving this vehicle in Port Huron, MI on January 23, 2017, as is more fully described below, paragraph 25.

24. Between January 19, 2017 and January 23, 2017, approximately 68 counterfeit checks were cashed or attempted to be cashed in the name of J.S. utilizing numerous social security numbers, at Walmarts located in Delaware, Pennsylvania, Ohio, Indiana, and Michigan. Your affiant has reviewed surveillance photographs of these transactions and it appears that the individual conducting those transactions was BECOATE.

25. On or about January 23, 2017, BECOATE was arrested by officers with the St. Clair County Sheriff's Office located in Port Huron, MI. BECOATE had attempted to enter Canada, en route to Toronto, Ontario, and was stopped at the Canadian border crossing. Officers searched the rental vehicle that BECOATE was driving and recovered the following items:

- Approximately 76 counterfeit payroll checks in various names

- 192 pieces of blank payroll check stock
- 25 different fraudulent driver's licenses in various names
- \$8,028.00 in US Currency
- 2 Driver's licenses in the name of BECOATE
- A US Passport in the name of BECOATE
- 2 moving violation tickets from Louisiana dated November 30, 2016 and
- A Federal Express receipt showing the shipment of a package from Detroit, MI

26. St. Clair County Sheriff's Officers were able to obtain the Federal Express package shipped by BECOATE and obtained a search warrant for the contents. The package was found to contain the following:

- A HP Laserjet Printer
- 83 counterfeit payroll checks in the name of J.S. and
- 9 counterfeit driver's licenses in the name of J.S.

27. The counterfeit checks and driver's licenses that were recovered by the St. Clair County Sheriff's Office bore the same name, J.S., that BECOATE had used to pass counterfeit checks in Arkansas and Texas in early December 2016 and in Delaware, Pennsylvania, Ohio, Indiana and Michigan in the days prior to BECOATE's arrest at the United States/Canada border.

28. BECOATE was found guilty on the charges against him in St. Clair County and was incarcerated from January 2017 until September 2017. During this time, the counterfeit check cashing by other co-conspirators continued but BECOATE was not seen in Walmart videotapes or photographs.

29. In late September 2017, BECOATE was released from prison in St. Clair County, Michigan. Immediately after his release, beginning on September 30, 2017 through October 2, 2017, approximately 17 counterfeit checks were chased or attempted to be cashed in the names of D.W. and R.B. at Walmarts located in Ohio and Pennsylvania. Your affiant reviewed surveillance photographs of these transactions and it appears the individual conducting them was BECOATE. In addition, evidence shows that subject Jeffrey ROACH was the individual who picked BECOATE up from prison upon BECOATE's release, as is shown below in paragraphs 45 and 46.

30. On or about September 25, 2017, subject Jeffrey ROACH rented a vehicle from National Rental Car and returned it on or about October 19, 2017. According to National Rental Car records, the car was returned with 7,324 miles driven. In addition, surveillance photographs and video taken during this period at Walmarts in various states including Michigan, Ohio, and Pennsylvania depict ROACH cashing and attempting to cash counterfeit checks; in some instances ROACH is shown to be in the same Walmart stores as BECOATE.

31. On January 16, 2018, approximately nine counterfeit checks were cashed or attempted to be cashed in the name of M.A., at Walmarts located in Delaware. Your affiant reviewed surveillance photographs of these transactions and it appears the individual conducting them was BECOATE.

32. Continuing in January 2018, BECOATE was seen on videotapes and photographs cashing and attempting to cash counterfeit payroll checks at Walmarts in various places throughout the United States. Surveillance photographs and video depict BECOATE cashing checks using the names and social security numbers of other individuals.

JEFFREY ROACH

33. Investigation to date has shown that between January 2015 and January 2018, subject Jeffrey ROACH has rented 57 vehicles from National Car Rental and Enterprise Rent-a-Car at various locations throughout the United States. The following information was provided by or on behalf of ROACH to National and Enterprise Rent-a-Car to secure the vehicles:

- On all rental contracts, ROACH provided telephone numbers 301-443-1909 and 301-543-9405.
- On 53 rental contracts from January 2015 to December 2017, ROACH provided an email address of “**J_BLACK009@YAHOO.COM**”
- On 2 rental contracts from May 2016 to July 2016, ROACH provided an email address of “**BAM85AGA@GMAIL.COM**”
- The rentals were paid for with various credit and debit cards registered to ROACH.
- On all rental contracts, ROACH provided Maryland driver's license #R200-390-730-704.

34. Your affiant conducted a query with NCIC regarding Maryland driver's license #R200-390-730-704 and found it registered to ROACH at 8406 Hamlin Street, Lanham, MD.

35. Investigation to date has shown that between July 2014 and December 2017, ROACH made reservations for 37 flights on Southwest Airlines. The following information was captured by Southwest Airlines related to the flights reserved by or on behalf of ROACH:

- The following email addresses were provided to Southwest Airlines related to flights reserved by ROACH:
 - **JEFFREYROACH1985@GMAIL.COM (34 times)**

- **CRAZYSWAGG87@GMAIL.COM** (2 times)
 - **AHMADBECOATE@GMAIL.COM** (once)
 - **JLMILLER1286@GMAIL.COM** (once)
- Records provided by Southwest Airlines show that ROACH made reservations to fly with BECOATE on five occasions. It appears that on at least 3 occasions, BECOATE's email addresses, **CRAZYSWAGG87@GMAIL.COM** and **AHMADBECOATE@GMAIL.COM**, were the email addresses used during booking.
 - Records provided by Southwest Airlines show ROACH made reservations to fly with MILLER on one occasion. It appears that on at least one occasion, MILLER's email address, **JLMILLER1286@GMAIL.COM**, was the email address used at booking.

COUNTERFEIT CHECK CASHING – ROACH

36. Investigation to date has shown that from on or about November 29, 2016 through on or about December 19, 2017, subject Jeffrey ROACH has cashed or attempted to cash over 1,000 counterfeit checks at various Walmarts across the United States. Walmart security has provided information on checks that were cashed or attempted to be cashed, along with surveillance photographs and videotapes of the transactions. As described below, several of the counterfeit checks that were cashed or attempted to be cashed coincided with flights taken by ROACH and vehicles rented by ROACH.

37. For example, on or about November 29, 2016, ROACH traveled on Southwest Airlines from BWI Airport to Dallas Airport. Records obtained from Southwest Airlines show

that at the time of the reservation, Southwest Airlines was provided with an email address of **"JEFFREYROACH1985@GMAIL.COM."**

38. On November 29, 2016, ROACH rented a vehicle from Dallas Airport from National Car Rental. Records obtained from National Car Rental show that at the time of the reservation, ROACH provided National Car Rental with an email address of **"J_BLACK009@YAHOO.COM,"** and further that the rental vehicle was returned by ROACH on December 9, 2016.

39. As previously noted above, in paragraphs 20 and 21, BECOATE also flew on Southwest Airlines and rented a vehicle from National Car Rental on the same date as ROACH, November 29, 2016.

40. Between November 29 and December 3, 2016, approximately 26 counterfeit checks were cashed or attempted to be cashed in the name of J.L. and M.L. at Walmarts located in Arkansas, Louisiana, and Texas. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting them was ROACH.

41. On or about February 1, 2017, ROACH rented a vehicle in Omaha, NE from National Car Rental. Records obtained from National Car Rental show that at the time of the reservation, National Car Rental was provided with an email address of **"J_BLACK009@YAHOO.COM,"** and further that the vehicle was returned by ROACH on February 4, 2017 in Denver, CO.

42. Between February 1, 2017 and February 3, 2017, approximately 83 counterfeit checks were cashed or attempted to be cashed in the name of J.L. at Walmarts located in Nebraska and Colorado. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting them was ROACH.

43. On April 11, 2017, ROACH rented a vehicle in Greensboro, NC from National Car Rental. Records obtained from National Car Rental show that at the time of the reservation, National Car Rental was provided with an email address of "J_BLACK009@YAHOO.COM," and further that the vehicle was returned by ROACH on April 18, 2017.

44. Between April 12, 2017 and April 17, 2017, approximately 44 counterfeit checks were cashed or attempted to be cashed in the name of C.W., K.W., R.L., and others at Walmarts located in Tennessee, Kentucky, and North Carolina. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting them was ROACH. During this same time period, and at the same Walmart locations where ROACH was seen cashing counterfeit checks, subjects Jared MILLER and Jethro RICHARDSON were also seen cashing counterfeit checks. This is more fully described below in sections pertaining to RICHARSON and MILLER, in paragraphs 56 and 70 respectively.

45. On September 25, 2017, ROACH rented a vehicle in Baltimore, MD from National Rental Car. Records obtained from National Car Rental show that at the time of the reservation, National Car Rental was provided with an email address of "J_BLACK009@YAHOO.COM," and further that the vehicle was returned by ROACH on October 19, 2017. According to National Rental Car records, the car was returned with 7,324 miles driven.

46. Between September 29, 2017 and September 30, 2017, approximately 34 counterfeit checks were cashed or attempted to be cashed in the name of J.N., D.W., E.H., and M.S. at Walmarts located in Michigan and Ohio. Your affiant reviewed the surveillance photographs of these transactions and it appears that the individual conducting them was

ROACH. As discussed above in paragraph 29, evidence shows BECOATE and ROACH cashing counterfeit checks during this same time frame at the same Walmart locations in Ohio.

47. On December 4, 2017, ROACH traveled on Southwest Airlines from BWI Airport to Minneapolis-St. Paul International Airport. Records obtained from Southwest Airlines show that at the time of the reservation, Southwest Airlines was provided with an email address of “**JEFFREYROACH1985@GMAIL.COM.**”

48. Also on December 4, 2017, ROACH rented a vehicle at Minneapolis-St. Paul International Airport, from National Car Rental. Records obtained from National Car Rental show that at the time of the reservation, National Car Rental was provided with an email address of “**J_BLACK009@YAHOO.COM,**” and further that the vehicle was returned by ROACH on December 6, 2017 at Midway Airport in Chicago, IL.

49. On December 6, 2017, approximately 10 counterfeit checks were cashed in the name of G.G. at Walmarts located in Illinois. Your affiant reviewed the surveillance photographs of these transactions and it appears that the individual conducting them was ROACH.

JETHRO RICHARDSON

50. Investigation to date has shown that between March 2011 and February 2018, subject Jethro RICHARDSON made reservations for 62 flights on American Airlines and US Airways. The following information was captured by American Airlines/US Airways related to the flights reserved by or on behalf of RICHARDSON.

- The following email addresses were provided to American Airlines/US Airways related to flights reserved by or for RICHARDSON:
 - **JAX.BLACK51@YAHOO.COM (18 times)**

o RICHARDSON_JAI@YAHOO.COM (22 times)

- Records provided by American Airlines and US Airways show that RICHARDSON made or had made on his behalf, reservations to fly with ROACH on at least four occasions. It appears that on at least one occasion, ROACH's email address, **JEFFREYROACH1985@GMAIL.COM**, was the email address used during booking.
- Records provided by American Airlines and US Airways show that RICHARDSON made or had made on his behalf, reservations to fly with HARVEY on at least one occasion. It appears that on this occasion, HARVEY's email address, **JUQUANANTHONY@GMAIL.COM**, was the email address used during booking.

COUNTERFEIT CHECK CASHING – RICHARDSON

51. The investigation to date has shown that subject Jethro RICHARDSON has cashed or attempted to cash approximately 454 counterfeit checks from on or about January 17, 2017 to on or about December 1, 2017. Walmart security has provided information on the counterfeit checks that were cashed or attempted to be cashed, along with surveillance photographs and video of the transactions. Several of the counterfeit checks that were cashed or attempted to be cashed coincide with flights taken by RICHARDSON.

52. For example, on January 28, 2017, RICHARDSON traveled on American Airlines from Charlotte, NC to Detroit, MI. Records obtained from American Airlines show that at the time of the reservation, American Airlines was provided with an email address of **“JAX.BLACK51@YAHOO.COM.”**

53. On January 29, 2017, approximately 14 counterfeit checks were cashed or attempted to be cashed in the names of C.E. and J.W. at Walmarts located in Michigan and Indiana. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting the transactions was RICHARDSON.

54. On January 30, 2017, RICHARSON traveled on American Airlines from Detroit, MI to Phoenix, AZ. Records obtained from American Airlines show that at the time of the reservation, American Airlines was provided with an email address of **"JAX.BLACK51@YAHOO.COM."**

55. On January 30, 2017 and January 31, 2017 approximately ten counterfeit checks were attempted to be cashed in the name of C.E., at Walmarts located in Arizona, Colorado, and New Mexico. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting the transactions was RICHARDSON.

56. Between April 14 and April 17, 2017, approximately 14 counterfeit checks were cashed or attempted to be cashed in the names of T.W. and C.C. at Walmarts located in Tennessee and North Carolina. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting the transactions was RICHARDSON.

57. On December 1, 2017, RICHARDSON traveled on American Airlines from Charlotte, NC to Chicago, IL. Records obtained from American Airlines show that at the time of the reservation, American Airlines was provided with an email address of **"JAX.BLACK51@YAHOO.COM."**

58. On December 1, 2017, approximately 15 counterfeit checks were cashed or attempted to be cashed in the names of J.M., T.W., D.E., B.W., J.L., J.E., AND W.R. at Walmarts located in Wisconsin and Minnesota. Your affiant reviewed surveillance photographs

of these transactions and it appears the individual conducting the transactions was RICHARDSON.

JUQUAN HARVEY

59. The investigation to date has shown that subject Juquan HARVEY has cashed or attempted to cash approximately 132 counterfeit checks from on or about January 7, 2017 to on or about October 7, 2017. Wal-Mart security has provided information on the cashed/attempted cashed checks along with surveillance photographs and video of the transactions. Several of the counterfeit checks that were cashed or attempted to be cashed coincide with flights taken by HARVEY.

60. A review of federal court records in the Eastern District of Virginia shows that during the time that he was committing these offenses, subject Juquan HARVEY was on federal supervised release for similar offenses. Those records show that on March 13, 2012, a ten-count criminal indictment was filed against HARVEY, under number 4:12CR22, for conspiracy to commit bank fraud and to possess and utter counterfeit securities of organizations (one count); bank fraud (five counts) and possessing and uttering counterfeit securities (four counts), in violation of 18 U.S.C. §§ 371, 1344 and 513(a), respectively. The docket in Criminal No. 4:12CR22 shows further that after pleading guilty to the charges HARVEY was sentenced on January 23, 2013 to 30 months in prison followed by three years of supervised release. The docket shows further that the U.S. Probation Office has filed a petition for violation of supervised release, alleging that HARVEY was out of the district without permission, the hearing on which is scheduled to be held Monday April 30, 2018.

61. Returning to travel by HARVEY and the email addresses given to airlines and car rental agencies in connection with that travel, for example, between August 12, 2015 and

January 30, 2018, HARVEY or someone acting on his behalf made reservations for HARVEY to take two flights on Southwest Airlines and 14 flights on American Airlines/US Airways. The following information was captured by Southwest Airlines and American Airlines/US Airways related to the flights reserved by or for HARVEY:

- The following email addresses were provided to Southwest Airlines and American Airlines/US Airways related to flights reserved by or for HARVEY:
 - **JUQUANANTHONY@GMAIL.COM** (6 times)
 - **JEFFREYROACH1985@GMAIL.COM** (2 times)
 - **VINCENTEWATSON@GMAIL.COM** (once)
- Records provided by American Airlines/US Airways show that HARVEY or someone acting on his behalf made reservations for HARVEY to fly with ROACH on three occasions. It appears that on at least two of those occasions, ROACH's email address, **JEFFREYROACH1985@GMAIL.COM**, was the email address used during the booking.
- Records provided by American Airlines/US Airways show that HARVEY or someone acting on his behalf made reservations for HARVEY to fly with RICHARDSON on one occasion.

62. On January 30, 2017, HARVEY traveled on American Airlines from Detroit, MI to Phoenix, AZ. Records obtained from American Airlines show that at the time of the reservation, HARVEY or someone acting on his behalf provided American Airlines with an email address of "**JUQUANANTHONY@GMAIL.COM**."

63. Prior to this flight, on January 29, 2017, approximately nine counterfeit checks were cashed/attempted to be cashed in the name of W.N. at Walmarts located in Indiana and

Michigan. Your affiant reviewed surveillance photographs and video of these transactions and it appears that the individual conducting the transactions was HARVEY.

64. After the flight to Phoenix, between January 30, 2017 and January 31, 2017, approximately eight checks were attempted to be cashed in the name of W.N. at Walmarts located in Arizona, New Mexico, and Colorado. Your affiant reviewed surveillance photographs and video of these transactions and it appears that the individual conducting the transactions was HARVEY.

65. On September 30, 2017, approximately 15 counterfeit checks were cashed or attempted to be cashed in the name of G.F. and D.W. at Walmarts located in Delaware. Your affiant reviewed surveillance photographs and video of these transactions and it appears that the individual conducting the transactions was HARVEY.

JARED MILLER

66. In March 2017, subject Jared MILLER rented one vehicle from Enterprise Rent-a-Car at a Columbus, OH rental location. The following information was provided by MILLER to Enterprise Rent-a-Car to secure the vehicle:

- MILLER provided a telephone number of 336-509-1081
- MILLER provided an email address of "BRICE557@YAHOO.COM"
- MILLER provided Ohio driver's license #UJ848407 to rent the vehicle.

67. Your affiant conducted a query with NCIC regarding Ohio driver's license #UJ848407 and found that this license was registered to MILLER at 1236 Fountain Lane, Apt. E, Columbus, OH.

68. Between July 2014 and October 2016, MILLER or someone acting on MILLER's behalf made reservations for 13 flights on Southwest Airlines. The following information was captured by Southwest Airlines related to flights reserved for MILLER:

- The following email addresses were provided to Southwest Airlines related to flights reserved for MILLER:
 - JLMILLER1286@GMAIL.COM (6 times)
 - MOCHABOY69@GMAIL.COM (3 times)
 - CRAZYSWAGG87@GMAIL.COM (2 times)
 - AHMADBECOATE@GMAIL.COM (once)
 - MALL3412@AOL.COM (once)
- Records provided by Southwest Airlines show that MILLER, or someone acting on his behalf, made reservations for MILLER to fly with BECOATE on two occasions.

COUNTERFEIT CHECK CASHING – MILLER

69. The investigation has determined that MILLER has cashed or attempted to cash more than 40 counterfeit checks from April 17, 2017 through May 1, 2017. Walmart security has provided information on the counterfeit checks that were cashed or attempted to be cashed, along with surveillance photographs and video from the transactions.

70. Between April 17, 2017 and April 20, 2017, approximately 14 counterfeit checks were cashed in the name of K.W. at Walmarts in North Carolina. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting the transactions was MILLER.

71. On May 1, 2017, approximately 10 counterfeit checks were cashed or attempted to be cashed in the name of K.W. at Walmarts located in North Carolina. Your affiant reviewed surveillance photographs of these transactions and it appears that the individual conducting the transactions was MILLER.

SUMMARY

72. Since approximately June of 2016, thousands of counterfeit payroll checks have been cashed or attempted to be cashed by a group of individuals, who have traveled to more than 35 different states and dozens of different Walmart locations within those states. These individuals have acquired the identities of numerous individuals, to include their name, date of birth, and Social Security Number, and have used this personal identifying information to obtain fraudulent identification cards. With this information, these individuals have successfully participated in a scheme to defraud by presenting counterfeit payroll checks bearing the names of the compromised individuals, containing the routing numbers of real banks and the bank account numbers of actual businesses that were allegedly drawn on banks that did not in fact issue the checks. Based on investigation to date, these individuals have caused a loss to Walmart of approximately \$494,297.00 and an intended loss of approximately \$831,743.00. The investigation to date has determined that subjects Ahmad BECOATE, Jeffrey ROACH, Jethro RICHARDSON, JARED MILLER and Juquan HARVEY and others known and unknown are willing participants in this scheme and have collaborated with at least one other person in the conspiracy. These individuals are using various methods to travel to the different jurisdictions to pass the counterfeit checks, including air travel and vehicle travel with several different companies. Furthermore, legitimate email addresses are being providing by the suspects to these companies confirming the travel arrangements. The investigation shows that to make travel

arrangements, the Ahmad BECOATE email address ahmad.becoate@gmail.com was used approximately 10 times, most recently on January 19, 2017; the Ahmad BECOATE email address Mall3412@aol.com email address was used approximately 29 times, most recently on October 26, 2016; and the Ahmad BECOATE email address Crazyswagg87@gmail.com email address was used approximately 54 times, most recently on February 2, 2018. The Jeffrey ROACH email address j_black009@yahoo.com email address was used approximately 53 times, most recently December 19, 2017 and the Jeffrey ROACH email address Jeffreyroach1985@gmail.com was used approximately 38 times, most recently on December 6, 2017. The Jethro RICHARDSON email address Jax.black51@yahoo.com email address was used approximately 19 times, most recently on February 17, 2018. The Jared MILLER email address Jlmiller1286@gmail.com was used approximately 13 times, most recently on January 8, 2016 and the Jared MILLER email address Mochaboy69@gmail.com was used approximately 4 times, most recently on February 27, 2016. The JuQuan HARVEY email address juquananthony@gmail.com was used approximately 7 times, most recently on on Janaury 30, 2017. It is believed that other companies which the subjects are using to facilitate their criminal conspiracy could be found with a search of these target email accounts and, perhaps, communications with other co-conspirators coordinating travel plans and information.

TRAINING AND EXPERIENCE

73. Based on my training and experience, and the experience of other Inspectors and agents involved in this investigation, I know the following information regarding individuals involved in identity theft, credit card fraud, wire fraud and bank fraud:

- Individuals will often keep records obtained from their fraudulent applications and purchases, including but not limited to emails, emailed receipts, emailed

applications, etc. These documents are usually kept by the individual for future reference, months and even years after the accounts were opened, and are often stored in the email's inbox. Such information can remain in the email account almost indefinitely.

- Individuals who engage in identity theft frequently obtain individual victims' personal and financial information through the theft or diversion of mail, the theft of personal property, the interception of Internet transactions, compromising personal information files from a legitimate business source, or purchasing the information through the "Dark Web." This information is stored in areas for ready access and to conceal them from law enforcement. I also know that persons who commit multiple acts of identity theft typically maintain documents related to those offenses for months and even years, in order to facilitate further fraud and theft. This information is often stored in email boxes so that it will be readily accessible from any computer or phone and so that it can be sent via email to other co-conspirators.
- Individuals who engage in identity theft often keep records or notations of personal and financial information of victims or intended victims. These records often include the victim's name, date of birth, social security number, driver's license number, true address, employment history and salary, mother's maiden name, true bank and credit account information. Individuals who commit multiple acts of identity theft and related crimes typically maintain records or notations of personal and financial information for months or even years after the information is obtained in order to facilitate further fraud and theft. This

information is often stored in email boxes so that it will be readily accessible from any computer or phone and so it can be sent via email to other coconspirators.

SERVICE AND EXECUTION

74. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. The statute permits law enforcement agents to serve it by fax or by mail upon AOL, Inc. I request that Oath Holdings, Inc. and Google, Inc., be required to produce the electronic communications and other information identified in Attachments A1 and A2 hereto. Because neither Oath Holdings, Inc. nor Google, Inc. is aware of the facts of this investigation, its employees are not in a position to search for relevant evidence. In addition, requiring Oath Holdings, Inc. and Google, Inc. to perform the search would be a burden upon the company. If all Oath Holdings, Inc. and Google, Inc. are asked to do is produce all the files in the account, an employee can do that easily. Requiring Oath Holdings, Inc. and Google, Inc. employees to search the materials to determine what content is relevant would add to their burden.

75. I request that the Court authorize law enforcement agents to seize only those items identified in Attachment B1 and B2 from what is produced by Oath Holdings, Inc. and Google, Inc. pursuant to the search warrant. In reviewing these messages, I will treat them in the same way as if I were searching a file cabinet for certain documents. E-mails will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

76. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

77. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue the warrant directing Oath Holdings, Inc. and Google, Inc. to comply even though neither Oath Holdings, Inc. nor Google, Inc. is located in this district, because the Court has jurisdiction over the offenses being investigated.

78. I also respectfully request that the warrant direct Oath Holdings, Inc. and Google, Inc. to produce log records and other non-content information pertaining to the subject email accounts. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under 18 U.S.C. 2703(c)(1)(A). Because I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth above to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

79. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email

communications, contacts list, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the Internet Protocol ("IP") addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

80. I further respectfully request that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrants, and the requisite inventory. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness. I further request, pursuant to

18 U.S.C. § 2705(b), that this Court direct Oath Holdings, Inc. and Google, Inc. not to notify any other person of this warrant until such time as the Court unseals it.

CONCLUSION


81. Based on the foregoing, I submit that there is probable cause that the items set forth in Attachments B1 and B2, which constitute evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 513 – uttering counterfeit securities; 18 U.S.C. § 1028 – credit card fraud; 18 U.S.C. § 1028A – aggravated identity theft; 18 U.S.C. § 1343 – wire fraud; 18 U.S.C. § 1344 – bank fraud; 18 U.S.C. § 371 – conspiracy to commit offenses against the United States (i.e., wire fraud, bank fraud, credit card fraud and uttering counterfeit securities); and 42 U.S.C. § 408 – Social Security fraud, are located in the aforementioned email accounts, which are hosted on servers owned, maintained, and/or operated by Google Inc., headquartered at 1600 Amphitheater Parkway, Mountain View, CA and Oath Holdings Inc., headquartered at 701 First Avenue, Sunnyvale, CA 94089.

82. Based upon the above stated information, I respectfully request that this Court issue warrants to search the nine subject email accounts, and that such search warrants be directed to Google Inc. and Oath Holdings Inc. for the purpose of searching the aforementioned email accounts.



SAMUEL A. BRACKEN
US Postal Inspector
US Postal Inspection Service

Sworn to before me this 4th day of
May, 2018:



MARILYN HEFFLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1 – LOCATION TO BE SEARCHED

(To be served on Google, Inc.)

This warrant applies to information associated with the Google Inc. user IDs and/or email addresses:

- **ahmadbecoate@gmail.com**
- **Crazyswagg87@gmail.com**
- **Jeffreyroach1985@gmail.com**
- **Jlmiller1286@gmail.com**
- **Mochaboy69@gmail.com**
- **juquananthony@gmail.com**

Which is stored at premises owned, maintained, controlled, and/or operated by Google Inc., headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043.

ATTACHMENT A2 – LOCATION TO BE SEARCHED

(To be served on Oath Holdings)

This warrant applies to information associated with the Oath Holdings Inc. user IDs and/or email addresses:

- **Mall3412@aol.com**
- **j_black009@yahoo.com**
- **Jax.black51@yahoo.com**

Which is stored at premises owned, maintained, controlled, and/or operated by Oath Holdings Inc., headquartered at 701 First Avenue, Sunnyvale, CA 94089.

ATTACHMENT B1

(This page to be served on Google, Inc.)

I. Information to be disclosed by Google, Inc. (the "Provider")

To the extent that the information described in Attachment A1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 18, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period of June 1, 2016 to the present:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;